The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/17/2009

SUBJECT:
Vulnerability in Adobe Shockwave Player Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Adobe Shockwave Player that could allow remote code execution. Adobe Shockwave Player is a widely used multimedia application used to display animations and video when visiting web sites. This vulnerability can be exploited by visiting a web page that contains a malicious Adobe Shockwave file. Successful exploitation may result in an attacker gaining the same privileges as the logged on user within the scope of the application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

Please note that there is no patch available for this vulnerability. Proof of concept code for a Denial-of-Service attack is publicly available but we have not received any reports of active exploitation.

SYSTEMS AFFECTED:

- All versions prior to and including Adobe Shockwave Player 11.5.1 601

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in Adobe Shockwave Player that could allow for remote code execution due to inadequate boundary checks on user-supplied data. This issue is triggered by passing an excessive amount of data to the 'PlayerVersion' property of the ActiveX control (swdir.dll), which is utilized to determine the version of Shockwave currently installed. This vulnerability can be exploited if a user visits a specially crafted web page designed to exploit this

vulnerability. Successful exploitation may result in an attacker gaining the same privileges as the logged on user within the scope of the application.. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

We have tested the proof of concept code and confirmed that it causes a Denial-of-Service (DoS) condition in Internet Explorer 8.

Please note that there is no patch available for this vulnerability. Proof of concept code for a Denial-of-Service attack is publicly available but we have not received any reports of active exploitation.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Adobe to vulnerable systems as soon as they become available.
- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Set the kill bit on the Class Identifier (CLSID) - {233C1507-6A77-46A4-9443-F871F945D258}; further instructions on how to set the kill bit can be found at the following location (http://support.microsoft.com/kb/240797).
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/36434

Microsoft:
http://support.microsoft.com/kb/240797